

Nr 1	Eis / nice to have Eis	Onderwerp Algemeen	Eis Alle informatiebeveiligingseisen uit het PvE maken integraal onderdeel uit van de overeenkomst en gelden gedurende de volledige looptijd van de opdracht.	BIO, CSIR, ISO control 5.20.01
2	Eis	Menselijk handelen	Opdrachtnemer borgt dat medewerkers en onderaannemers voorafgaand aan uitvoering van werkzaamheden geïnstrueerd zijn over minimaal: - omgang met toegang tot VRI-kasten; - gebruik van informatiesystemen van de gemeente Utrecht; - verbod op ongeautoriseerd aansluiten van apparatuur; - omgang met informatie en vertrouwelijkheid; - herkenning en melding van beveiligingsincidenten. Opdrachtnemer kan op verzoek van gemeente Utrecht aantonen dat deze instructie heeft plaatsgevonden, bijvoorbeeld door middel van instructiemateriaal, registraties of bevestigingen van medewerkers	BIO 5.04, 6.02, 6.03 CSIR hfdt 17
3	Eis	Personeel	Opdrachtnemer zet alleen medewerkers in die geschikt en betrouwbaar zijn voor de werkzaamheden en, indien van toepassing, meewerkt aan het overleggen van een VOG.	BIO 6.01
4.1	Eis	Toegang	Toegang tot VRI-kasten vindt uitsluitend plaats volgens door gemeente Utrecht vastgestelde toegangsprocedures. Sleutels, passen of andere toegangsmiddelen worden persoonlijk of aantoonbaar beheerst uitgegeven en mogen niet worden gedeeld.	CSIR hfdt 2.1
4.2	Eis	Toegang	Opdrachtnemer houdt een actueel overzicht bij van medewerkers die toegang hebben tot VRI-kasten en verstrekte toegangsmiddelen. Wijzigingen in deze toegang, het verlies of de diefstal van toegangsmiddelen en het einde van de inzet van medewerkers met toegang worden direct aan gemeente Utrecht gemeld.	BIO 5.18 CSIR hfdt 2.1
4.3	Eis	Toegang	Opdrachtnemer gebruikt voor informatiesystemen van gemeente Utrecht uitsluitend persoonlijk toegekende accounts. Het delen van accounts, wachtwoorden of andere authenticatiemiddelen is niet toegestaan.	BIO 5.16
4.4	Eis	Toegang	Opdrachtnemer werkt mee aan door gemeente Utrecht voorgeschreven authenticatiemaatregelen voor toegang tot informatiesystemen, zoals het gebruik van multi-factor authenticatie (MFA) indien dit wordt toegepast.	BIO 5.17
5.1	Eis	Gebruik van apparatuur / informatiesystemen	Opdrachtnemer gebruikt toegang tot gemeentelijke informatiesystemen, objecten (VRI-kasten) en opdrachtinformatie uitsluitend voor de uitvoering van de opdracht en alleen voor medewerkers die deze toegang nodig hebben.	ISO 5.10, 5.15
5.2	Eis	Gebruik van apparatuur / informatiesystemen	Opdrachtnemer mag geen laptop, mobiel apparaat, USB-apparaat of andere apparatuur aansluiten op UTP-poorten, netwerkpoorten, VRI-toestellen of andere digitale interfaces, tenzij gemeente Utrecht dit vooraf schriftelijk heeft toegestaan. Aan een eventuele toestemming kan gemeente Utrecht aanvullende beveiligingsvoorwaarden verbinden.	CSIR hfdst 2.9
5.3	Eis	Gebruik van apparatuur / informatiesystemen	Apparaten waarmee opdrachtnemer toegang krijgt tot gemeentelijke informatiesystemen of waarop opdrachtinformatie wordt verwerkt, moeten passend zijn beveiligd. Dit houdt minimaal in dat deze apparaten zijn voorzien van actuele beveiligingsupdates, malwarebescherming, schermvergrendeling en toegangsbeveiliging. Gemeente Utrecht kan op verzoek, bij een beveiligingsincident of bij gerede twijfel aantoonbaarheid hiervan vragen.	ISO 7.9 en 8.1
6.1	Eis	Incidentmanagement	Opdrachtnemer zorgt dat alle betrokken medewerkers voor aanvang van de werkzaamheden bekend zijn met de door meldprocedure van de gemeente Utrecht voor beveiligingsincidenten en weten welke situaties zij moeten melden.	BIO 5.24, 6.08
6.2	Eis	Incidentmanagement	Opdrachtnemer meldt beveiligingsincidenten, verlies van toegangsmiddelen, onbevoegde toegang, onbekende apparatuur/bekabeling in VRI-kasten, misbruik van accounts of datalekken onverwijld aan gemeente Utrecht.	BIO 5.20.05
6.3	Eis	Incidentmanagement	Opdrachtnemer werkt mee aan onderzoek, herstel en evaluatie bij beveiligingsincidenten die verband houden met de opdracht. Op verzoek levert opdrachtnemer relevante informatie aan over betrokken medewerkers, tijdstippen, werkzaamheden en gebruikte middelen.	CSIR hfdst 2.3
7	Eis	Recht op audit	Opdrachtnemer moet op verzoek kunnen aantonen dat aan de relevante beveiligingseisen wordt voldaan, bijvoorbeeld met procedures, registraties, instructies, bewijs van training, toegangsregistraties of incidentrapportages. Gemeente Utrecht heeft het recht om naleving steekproefsgewijs te controleren.	BIO 5.20
8	Eis	Exit	Bij beëindiging van de opdracht levert opdrachtnemer alle door gemeente Utrecht verstrekte toegangsmiddelen, documentatie en gemeentelijke informatie in. Daarnaast meldt opdrachtnemer welke medewerkers en onderaannemers geen toegang meer nodig hebben tot gemeentelijke informatiesystemen en fysieke objecten, zodat gemeente Utrecht toegangsrechten en toegangsmiddelen kan beëindigen of intrekken.	BIO 5.20.06
9	Eis	Onderaannemers	Opdrachtnemer zorgt voor volledige ketentransparantie door toeleveranciers aan de opdrachtgever bekend te maken, de eisen van de opdrachtgever door te leggen aan deze toeleveranciers, aantoonbaar inzicht te bieden in de beveiliging van de gehele leveranciersketen, en een helder subverwerkersbeleid te voeren waarin wordt vastgelegd welke derden data verwerken en waarin tijdige kennisgeving bij wijzigingen (met name bij SaaS- en cloudtoepassingen) is geborgd.	BIO 5.21